Pasadena Citizens' Advisory Council

www.pasadenacac.org

Summary of
Thursday, December 1, 2016 Meeting

FBI ON CYBER SECURITY

FBI Computer Scientist James Morrison, a member of the FBI's Houston Cyber Task Force, talked to PCAC about cyber security risks and what the FBI does to address them. He also made suggestions for cyber safety for both individuals and business. Highlights follow:

SMART PHONES

- Remember that your smart phone is a computer and more powerful than the one used to land men on the moon.
- Business cyber security policies need to consider that workers are using their personal phones on your corporate network.

CYBER ATTACKS

- Cyber attacks will not go away. It is easy to attack. Either you've been hacked and know it or hacked and unaware. Virtually every country has cyber attack capability.
- Attacks often begin with universities because they have high speed Internet connectivity.
- Attacks are made internationally by countries and criminal enterprises. Domestically, they come from criminal enterprise and others, like hacktivists who hack for political gain. Insider threats are the other source of attacks.
- About 40% of threats to business cyber security come from current or former employees. Prevent those being laid off from doing damage before they leave. Cyber security requires good general security operations, such as noticing a pattern of someone staying late without a good reason.

CYBER THREATS

- Website defacing can be the start of an attack by giving a virus to all who visit your website, which ruins your reputation. Change your website design periodically.
- Denial-of-service attacks can put viruses into "the Internet of things" that are connected to the Internet, like web cameras.
- About 95% of attacks are phishing, where someone pretends to be a legitimate business. Businesses should conduct tests to see if workers know not to click on suspicious links. About 15% typically will do so even if they know to watch for such things because we feel compelled to click because we use a computer mouse and have been "trained" to do so.
    - Spear phishing targets a specific company or person. Linked In is a good resource for a criminal to find who works at a company.

    - Whaling is aiming for a big fish, like a CEO.
    - Vishing is voice phishing; e.g. "This is the IRS calling."
- Avoid putting staff directories on your website.
- Domain twisting means someone creates a website that looks like a real one at first glance; e.g. We11s Fargo, spelled with two number 1s instead of two Ls. Companies who anticipate the twist may buy that domain so no one else does. Don't let your domain name lapse or someone else may pick it up.
- Ransomware is currently a big problem. Most cases are attacks on home computer users. About 10% of the time, the criminals will give you your data back, but individuals are finding their data held for ransoms up to $1000 at times. Be sure you are backing up your data. Then you can ignore the ransom threat. But don't keep your external hard drive plugged in all the time or it can be affected too.
- It is not enough for a business itself to have security practices. Its vendors must also do so or they can be the entrée into your system.
- Nothing keeps you totally safe but the precautions you take will make you a harder target to damage.
- Sometimes when data are taken, they are held for a very long time before anyone tries to use them.
- Good antivirus software catches about 20% of viruses. But it only works if you install it and update it.
- Your WiFi box comes with a password printed on the box. Change it!
- SCADA systems that are used to control plant operations and pipelines are not hooked to the Internet, but a USB drive with a virus could get into that system. In one cyber security drill, a number of USB drives were dropped in a parking lot to see if people would pick them up and plug them in to see what was on them. Too many people did.

PASSWORDS

- Create good passwords and change patterns often. Avoid significant dates in your life, your pets' names, relatives' names, your school, etc. Don't use real words. Avoid always starting a password with a capital letter and ending with a 1 or 2; this is a very common pattern.
- Don't use the same password for everything. Use a Password Manager so you can have many different ones and not have to memorize them all. Cloud-based password managers invest millions in security and have not yet had major breaches. Last Pass is an example of a cloud-based password manager.
- When asked to provide your mother's maiden name as a security question, don't feel obligated to be truthful.
- Don't overshare on social media. Be especially careful about posting photos of your children and grandchildren.

WI-FI SAFETY

- Don't use free hotel WiFi for anything personal. Hotels rarely change the password. At DefCon, the hackers convention held annually in Las Vegas (and attended by "the good, the bad, and the in between"), organizers traditionally show the hotel's WiFi on the conference room screen --

and who's logged on-- and call them "sheep." A personal hotspot is a safer way to get to the Internet when you travel.

- Be careful about those airport hotspots where you can recharge your devices. Look for the other end of the cord and be sure it's not going into the computer of someone sitting nearby and "juice jacking."
- If you leave Bluetooth on all the time, encrypt your phone and data.
- Don't "jailbreak" your phone.
- Engage on social media only with people you know and trust.

COMPLAINTS AND INFRAGARD

- Internet crime complaints may be registered at www.IC3.gov.
- Infragard is a partnership between the FBI and the private sector that companies should consider joining. One of their services is to share information about new threats. Apply online at https://www.infragard.org